SAJTÓKÖZLEMÉNY

A Szegedi Tudományegyetem közreműködésével fejleszt a Balasys IT Kft. korszerű technológiákat ötvöző, ipari környezetre optimalizált kiberbiztonsági feladatokat ellátó hálózati védelmi megoldásokat. A konzorcium az NKFIH Alapból a 2020-1.1.2-PIACI-KFI keretében 765 164 369 Ft támogatást elnyert 2020-1.1.2-PIACI-KFI-2020-00114 szerződés számú, „CyGWICS - Ipari környezetre optimalizált kiberbiztonsági feladatokat ellátó hálózati átjáró eszköz fejlesztése" c. projektjét 2021.01.01. napján megkezdte.

A projekt szakmai összefoglalója:

Az ipari automatizálási és folyamatirányítási rendszerek (ICS/SCADA) informatikai biztonsága egyre fontosabb kihívást jelent. Egyfelől ezek a rendszerek kritikus infrastruktúráink (pl. energia- és ivóvízellátás, közlekedés) és gazdasági termelésünk (gyártás, feldolgozás) alapját képezik, másfelől ezeket a rendszereket hálózatba kapcsolt programozható berendezések alkotják, amelyek a hálózati munkaállomásokhoz hasonlóan számos sérülékenységgel rendelkeznek, és a klasszikus támadási módokon túl további felületet nyitnak az ezzel visszaélni szándékozók számára. Az ICS rendszerek elleni támadásnak fizikai következményei is lehetnek, amelyek a berendezések meghibásodásához, a rendszer által nyújtott kritikus szolgáltatások vagy termelési és feldolgozási folyamatok leállásához vezethetnek, ezzel jelentős anyagi veszteséget okozva. Az üzembiztonságot szolgáló alrendszerek támadása személyi sérüléshez vagy környezetkárosításhoz is vezethet, melyek az anyagi veszteségen túl az emberi életben is jóvátehetetlen következményekkel járhat.

Az ICS/ SCADA rendszereket üzemeltetők körében erős piaci igény mutatkozik olyan biztonsági megoldásokra, melyek jól illeszthetők a már meglévő ICS/SCADA rendszerekhez, azokban csak minimális változtatást igényelnek, nem zavarják a funkcionális és üzembiztonsági követelmények kielégítését, könnyen bevezethetők és jól menedzselhetők.

Jelen projektben egy a fenti igényeket kielégítő megoldás, az ipari környezet sajátosságaihoz illeszkedő hálózati átjáró eszköz kerül kifejlesztésre, mely alkalmas egyrészt a rendszer különböző zónái közötti hálózati forgalom elemzésére és szűrésére, másrészt az eszköz által védett zónán belüli hálózat forgalmának elemzésére és támadásra utaló anomáliák észlelésére. A projektben kifejlesztésre kerülnek a megvalósításhoz szükséges algoritmusok, az azokat megvalósító szoftverrendszerek, valamint a kifejlesztett szoftverrendszerek futtatására alkalmas platform. A projektben külön figyelmet kap magának a platformnak az informatikai biztonsága. A projektben továbbá új, gépi tanulásra épülő forgalom elemzési és anomália azonosítási megoldások kerülnek kifejlesztésre, melyek adaptálhatóvá teszik az átjárót különböző ipari környezetekhez.

A projekt teljes futamideje kettő év, minden év végén egy mérföldkővel. A kutatás-fejlesztési feladatokban a konzorciumi partnerek együttműködnek, ugyanakkor minden főbb komponensnek megvan a saját felelőse. Az SZTE az ipari hálózati anomália azonosítást végző szoftverrendszerre és a gépi tanulás területén ehhez szükséges elméleti kutatásra, valamint a validációs feladatokra összpontosít.

A kutatási folyamatok 2021. 01. 01-jén kezdődnek és 2022. 12. 31-ig tartanak.

NEMZETI KUTATÁSI, FEJLESZTÉSI ÉS INNOVÁCIÓS HIVATAL

AZ NKFI ALAPBÓL MEGVALÓSULÓ PROJEKT